SELinux vs. AppArmor – Vergleich der Linux-Sicherheitsmodule

Inhaltsverzeichnis

SELinux und AppArmor sind Linux-Sicherheitsmodule zur Zugriffskontrolle. Während SELinux durch Mandatory Access Control (MAC) höchste Sicherheit bietet, ist AppArmor eine einfachere, profilbasierte Lösung. SELinux ist ideal für Hochsicherheitsumgebungen, AppArmor hingegen für Benutzer mit einfacherem Sicherheitsbedarf.

SELinux (Security-Enhanced Linux) und **AppArmor (Application Armor)** sind zwei weit verbreitete **Linux-Sicherheitsmodule (LSMs)**, die den Zugriff von Prozessen und Anwendungen auf das System kontrollieren. Beide bieten eine **zusätzliche Sicherheitsschicht**, unterscheiden sich jedoch in ihrer **Funktionsweise und Verwaltung**.

1 Was ist SELinux?

SELinux ist ein **Mandatory Access Control (MAC)-System**, das den Zugriff von Prozessen, Benutzern und Anwendungen auf Dateien und Systemressourcen strikt regelt.

1.1 Merkmale von SELinux

- **Fein granulare Kontrolle über Prozesse und Dateien**.
- **Policy-basierte Sicherheit**, die Zugriffe über **Labels** und **Kontexte** definiert.
- **Standardmäßig in Red Hat-basierten Distributionen enthalten** (RHEL, CentOS, Fedora).
- **Drei Modi**:
  - **Enforcing** (Regeln werden strikt durchgesetzt).
  - **Permissive** (Regeln werden protokolliert, aber nicht durchgesetzt).
  - **Disabled** (SELinux ist deaktiviert).

1.2 Vorteile von SELinux

- **Höhere Sicherheit durch Mandatory Access Control (MAC)**.
- **Fein abstimmbare Policies für hochsichere Umgebungen**.
- **Erkennt und blockiert Exploits automatisch**.

1.3 Nachteile von SELinux

- **Komplexe Verwaltung und Konfiguration**.
- **Erfordert tiefere Kenntnisse über Linux-Sicherheitsmechanismen**.
- **Kann Anwendungen unerwartet blockieren, wenn Policies nicht korrekt konfiguriert sind**.

2 Was ist AppArmor?

AppArmor ist ein **leichtgewichtiges MAC-System**, das Sicherheitsrichtlinien für Programme definiert und deren Zugriff auf Systemressourcen einschränkt.

2.1 Merkmale von AppArmor

- **Profile-basierte Zugriffskontrolle**, die Prozesse auf erlaubte Aktionen beschränkt.
- **Einfachere Verwaltung im Vergleich zu SELinux**.
- **Standardmäßig in Debian- und Ubuntu-basierten Distributionen enthalten**.
- **Modi zur Steuerung der Sicherheitsrichtlinien**:
  - **Enforced** (Regeln werden strikt durchgesetzt).
  - **Complain** (Regeln werden protokolliert, aber nicht durchgesetzt).

2.2 Vorteile von AppArmor

- **Einfachere Verwaltung durch vordefinierte Profile**.
- **Weniger aufwendig in der Konfiguration als SELinux**.
- **Gute Integration in Debian, Ubuntu und SUSE Linux**.

2.3 Nachteile von AppArmor

- **Weniger fein granulare Kontrolle als SELinux**.
- **Nicht so umfassend für hochsichere Umgebungen**.
- **Weniger standardisierte Profile für spezifische Anwendungen**.

3 Vergleich: SELinux vs. AppArmor

Kriterium	SELinux	AppArmor
Sicherheitsmodell	Mandatory Access Control (MAC)	Profile-basierte Zugriffskontrolle
Komplexität	Hoch	Mittel
Konfigurationsaufwand	Erfordert tiefgehendes Verständnis	Leicht anpassbar mit einfachen Profilen
Standardmäßig in	Red Hat, CentOS, Fedora	Debian, Ubuntu, SUSE
Flexibilität	Sehr granular	Weniger flexibel als SELinux
Logging	Detaillierte Protokolle	Weniger umfangreiche Logs

4 Wann sollte SELinux oder AppArmor verwendet werden?

- **SELinux ist geeignet für:**
  - Hochsichere Umgebungen mit strengen Zugriffskontrollen.
  - Enterprise- und Server-Systeme mit sensiblen Daten.
  - Nutzer, die eine **präzise und granulare Kontrolle** benötigen.
- **AppArmor ist geeignet für:**
  - Desktop-Systeme oder Server mit mittleren Sicherheitsanforderungen.
  - Nutzer, die eine **einfache Verwaltung und schnelle Konfiguration** bevorzugen.
  - Anwendungen, die ohne tiefgehende Anpassung geschützt werden sollen.

5 Alternativen zu SELinux und AppArmor

- **Grsecurity** – Erweiterter Kernel-Patch für hochsichere Umgebungen.
- **Tomoyo Linux** – Alternative MAC-Implementierung mit einfacher Policy-Verwaltung.
- **SMACK** – Weniger verbreitet, aber in Embedded-Systemen genutzt.

6 Fazit

SELinux und AppArmor sind zwei unterschiedliche Ansätze zur **Zugriffskontrolle unter Linux**. Während SELinux eine **fein granulare Kontrolle** für Hochsicherheitsumgebungen bietet, ist AppArmor **einfacher zu verwalten und ideal für Desktop- und Standard-Server-Umgebungen**.